IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Massimiliano Antonio Poletto et al.	Art Unit	: 2134
Serial No.	: 10/066,252	Examiner	: Andrew L. Nalven
Filed	: January 31, 2002	Conf. No.	: 2792
Title	: ARCHITECTURE TO THWART DENIAL OF SERVICE ATTACKS		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Pursuant to 37 C.F.R. § 41.41, Applicant responds to the Examiner's Answer, as follows

Claims 1 and 5

The examiner argues that: "**Mansfield teaches a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link).**" The examiner contends that this feature is met because: "**Mansfield teaches ... traffic monitors disposed on network connections (Mansfield, Page 6, Figure 4). Each traffic monitor examines traffic entering or leaving sites (data centers) by collecting relevant packet count information from each link connecting each site/data center (Mansfield, Page 6, Section 3.1).**" Appellant disagrees.

Appellant responds that Mansfield does not teach "a device, coupled to physical links between the data center and a network ..., that ... collects statistical information on packets that are sent between the network and the data center ... for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to." For example, there is no description of a provisioned device described in Mansfield.

The examiner further contends that:

> **Finally, Mansfield teaches that the collection of statistical information on packets occurs as if the device was disposed on links that are downstream from the links that the provisioned monitor is coupled to (Mansfield, page 6 Section 3.1, traffic monitors traffic entering each site). Mansfield teaches the cited limitation**

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: February 06, 2008

by teaching the traffic monitor disposed on the network link entering each site (Mansfield, Page 6, Figure 4).

The traffic monitor collects packet count information from the link it is disposed on (Mansfield, page 6 Section 3.1, Figure 4). Because all packet count information for the link is collected including traffic entering and leaving the data center (see Mansfield, Page 7, Section 3.4, echo and response packets), Mansfield's traffic monitor acts as if it is disposed on links that are downstream. When data flows downstream from the sites the data flows out from a site into the network. Mansfield's traffic monitors collect packet count information on traffic on this link and thus Mansfield teaches that the collection of statistical information on packets occurs as if the device was disposed on links that are downstream from the links that the provisioned monitor is coupled to.

This explanation of how Mansfield teaches this feature of: "examining traffic as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to," is not supported by any reasonable reading of Mansfield. In 3.1, Mansfield does not describe any differentiation in collection, much less a differentiation based on a plurality of customers. Mansfield merely provides for each traffic monitor a single count for all packets seen by that traffic monitor.

Indeed, Mansfield at 3.1, teaches away from the claimed feature "a device coupled to physical links between the data center and the network that collects statistical information by examining traffic" when Mansfield states: "**It should be noted that the information used is packet count only, neither packet capture nor analysis is needed.**"[1] By only using packet count, how can Mansfield examine traffic, as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to. Where can Mansfield provide a provisioned monitor by merely keeping a single packet count on each traffic monitor?

The thrust of the examiner's argument that: "**Because all packet count information for the link is collected including traffic entering and leaving the data center (see Mansfield, Page 7, Section 3.4, echo and response packets), Mansfield's traffic monitor acts as if it is disposed on links that are downstream.**", is unsupportable based on the teachings of Mansfield.

This reasoning is erroneous because if all Mansfield teaches is collecting all packet count information for the link, how does that act of collecting, as presented by the examiner, allow for "examining traffic as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to." As understood each link that is monitored would have but

[1] Mansfield 3.1 page 6.

one count of the number of packets that are seen by each traffic monitor. The claim however, requires that "the device was disposed on links that are downstream from links that the provisioned monitor is coupled to." The examiner argument addresses a feature of "devices disposed on links," however that is not what is claimed in claim 1. Moreover, even based on that reasoning, the examiner cannot show any teaching in Mansfield suggestive of a provisioned monitor, as claimed.

Therefore, the examiner fails to explicitly show where Mansfield teaches these features because Mansfield neither describes nor suggests the foregoing features. Because these features are not described by the disclosed traffic monitors of Mansfield, at Page 6, Section 3.1; Page 7, Section 3.4; Fig. 4, or elsewhere, Mansfield does not identically describe all of the features of the claim arranged as in the claim, and therefore Mansfield cannot be an anticipating reference.

Claims 11, 24, and 27

The examiner argues that:

> **... Mansfield teaches the provisioned monitor maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects information from link) and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8)." Mansfield teaches the cited limitation by teaching that each traffic monitor separately collects packet count statistics on the link on which it is disposed (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link). Thus, each monitor has a counter log that it maintains that pertains to each individual customer viewed by the Examiner as a site (Mansfield, Page 6, Figure 4, sites 1, 2, 3, 4).**
>
> **Mansfield teaches a global counter log that accounts for all traffic seen on the link by disclosing the combining of the counts from each traffic monitor that pertain to each site/customer (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).**

Claim 11 requires a provisioned monitor ... maintaining separate counter logs for each provisioned customer, and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to.

The examiner argues that these log features are met by "**Mansfield teaches the cited limitation by teaching that each traffic monitor separately collects packet count statistics on the link on which it is disposed (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link).**" Nothing in

Mansfield suggests that the "**separately collects packet count statistics on the link,**" is further defined as separate counter logs for each provisioned customer. As described by Mansfield, there is but one counter. "**It should be noted that the information used is packet count only, neither packet capture nor analysis is needed.**" Given this statement it is clear that each traffic monitor only collects information with one counter. Therefore, none of the traffic monitors meet the limitation of separate counter logs for each provisioned customer, which is specifically required by the claim, to wit, "a provisioned monitor ... maintaining separate counter logs for each provisioned customer."

The examiner argues that: "**Mansfield teaches a global counter log that accounts for all traffic seen on the link by disclosing the combining of the counts from each traffic monitor that pertain to each site/customer (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).**" Mansfield Fig. 6 is reproduced below:

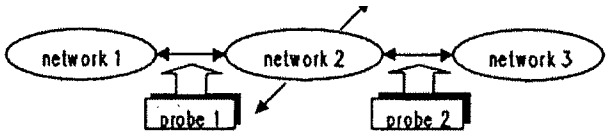

Fig. 6 Experiment environment

While, Mansfield combining counts from probe 1 and probe 2, can provide packet counts for all traffic seen by probe 1 and probe 2, the claim requires that "a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to." Probe 1 and Probe 2 are between two different networks, network 1 and network 2. Combining packet counts for all traffic seen by probe 1 and probe 2 combines the counts for two traffic monitors, monitoring two different networks and therefore does not meet the feature of a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to.", as in claim 11.

Claims 2, 3, 7, 9, 10, and 33

Claims 2 and 3 further limit claim 1 to the monitoring device being coupled to a control center through "a dedicated, private network."

The examiner relies on Crosbie to cure the deficiencies of Mansfield. Specifically, the examiner argues that: **Crosbie teaches the monitoring device being coupled to a control center through a dedicated**

private network (Crosbie, paragraph 0116-0118) by teaching an SSL connection between a management station and agent systems. The examiner further argues that: "**A secure point to point connection is a dedicated private network because a network is any combination of computer elements and in this case the network is dedicated to secure transmission of data between two predefined entities. Hence, Crosbie's SSL connection providing a secure dedicated connection between an IDS system (monitoring device) and the management station (Crosbie, paragraph 0118) meets the limitation of the monitoring device being coupled to a control center through a dedicated private network.**" Applicant contends that the features of a dedicated, private network is not be suggested by the SSL layer, which is a cryptographic protocol that provides secure communications on the Internet. While this layer is effective in providing secure transmission, it is not a private network nor a dedicated network, but merely another layer in the TCP/IP protocol.

Claim 7 explicitly includes the features of collecting, using a provisioned monitor, statistical information on packets that are sent between a network and a plurality of customers of the data center. Mansfield does not explicitly show this feature being performed by a provisioned monitor. Mansfield shows plural traffic monitors on plural links but not configured or arranged to collect "statistical information on packets that are sent between a network and a plurality of customers of the data center." As discussed in claim 1, Mansfield does not suggest the feature of: "examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on." Also, as discussed about the combination of Mansfield with Crosbie does not teach "... a dedicated network, to a control center.", by the SSL teaching of Crosbie.

Claims 4, 6, 12-15, 25, 28-32, and 34

The examiner argues that: "**... Mansfield teaches ... to install filters to thwart denial of service attacks ... (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach the monitoring device is a gateway device.**" The examiner uses Kim to cure the admitted deficiencies of Mansfield "**by teaching that a gateway device can be used as a monitoring device that installs filters (Kim, Abstract, integrated security gateway).**" The examiner argues that: "**Kim's gateway device acts to install filters in order to respond to security issues.**" Appellant contends that nothing in the purported combination of Mansfield and Kim is directed to the claimed feature. Kim merely using filters for security associations on packets and the examiner is merely proposing a re-naming of the traffic monitors

of Mansfield to call them gateways, as clearly evidenced by the examiner's argument that: "**While Kim's device is not specifically directed to thwarting denial of service attacks the principle is the same.**", Kim's gateway filters packets and allows packets based SA filtering rules, not network intrusions or DOS attacks.

The examiner's motivation "**... because it offers the advantage of reducing costs by integrating security elements and increasing security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).**", is also inadequate. The discussion relied on by the examiner here pertains to prior art and not to the integrated security gateway disclosed in the Abstract. These so called advantages are the result of the IDS's and VPN's disclosed as prior art, and apparently not specifically of the integrated security gateway.

Claims 6 and 12-15

Regarding claims 6 and 12-15, the examiner relied on the argument for claims 4 and 11 and did not specifically address the additional arguments raised by Appellant in the Appeal Brief, regarding the feature of "a process to aggregate traffic from the various links and to produce logs and detection heuristics." This is clearly taught away from by Mansfield's teachings "**It should be noted that the information used is packet count only, neither packet capture nor analysis is needed.**"[2]

Claims 29, 30-32 and 34

Regarding claims 29, 30-32 and 34, the examiner relied on the argument for claims 1 and 11 and did not specifically address the additional arguments raised by Appellant in the Appeal Brief, regarding the feature of "performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic."

Claim 8

Regarding claim 8, the examiner relied on the argument for claims 1 and 4.

---

[2] Id.

Claim 16

Regarding claim 8, the examiner relied on the argument for claims 4 and 11 and did not specifically address the additional arguments raised by Appellant in the Appeal Brief, regarding the feature of: "the gateway maintains duplicate packets, keeping both a global packet log and a packet log for each monitor."

According, for these reasons, and the reasons stated in the Appeal Brief, Applicant submits that the final rejection should be reversed.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 2/06/08

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21846211.doc